Terms used
communications and **unencrypted** and **transfer** and **protocol** and **subset** and **payload** **determin$4** and **secret**

Sort results by relevance

Display results expanded form

Save results to a Binder

Search Tips

Open results in a new window

Results 1 - 20 of 200

Result page: **1** 2 3 4 5 6 7 8 9

Best 200 shown

1 DISP: Practical, efficient, secure and fault-tolerant distributed data storage

Daniel Ellard, James Megquier
February 2005 **ACM Transactions on Storage (TOS)**, Volume 1 Issue 1

Publisher: ACM Press

Full text available: pdf(148.11 KB) Additional Information: full citation

DISP is a practical client-server protocol for the distributed storage of immutable data objects. between total storage space, computational overhead, and guarantees of availability, integrity, item is encoded, what level of integrity checks are computed and stored with each item, and w

Keywords: Distributed data storage

2 Unlinkable serial transactions: protocols and applications

Stuart G. Stubblebine, Paul F. Syverson, David M. Goldschlag
November 1999 **ACM Transactions on Information and System Security (TISSEC)**, Vol

Publisher: ACM Press

Full text available: pdf(184.87 KB) Additional Information: full citation

We present a protocol for unlinkable serial transactions suitable for a variety of network-based services. The protocol prevents the service from tracking the behavior of its customers, while p Our basic protocol structure and recovery protocol are robust against failure in protocol termina

Keywords: anoymity, blinding, cryptographic protocols, unlinkable serial transactions

3 Link and channel measurement: A simple mechanism for capturing and replaying wireless

Glenn Judd, Peter Steenkiste
August 2005 **Proceeding of the 2005 ACM SIGCOMM workshop on Experimental a**

Publisher: ACM Press

Full text available: pdf(6.06 MB) Additional Information: full citation

Physical layer wireless network emulation has the potential to be a powerful experimental tool. wireless channel. In this paper we examine the possibility of using on-card signal strength mea ubiquity with which these measurements can be obtained since virtually all wireless devices pro

Keywords: channel capture, emulation, wireless

4 Practical byzantine fault tolerance and proactive recovery

Miguel Castro, Barbara Liskov
November 2002 **ACM Transactions on Computer Systems (TOCS)**, Volume 20 Issue 4
Publisher: ACM Press
Full text available: pdf(1.63 MB) Additional Information: full citation

Our growing reliance on online services accessible on the Internet demands highly available sy malicious attacks are a major cause of service interruptions and they can cause arbitrary beha to build highly available systems that tolerate Byzantine faults. BFT can be used in practice to i

Keywords: Byzantine fault tolerance, asynchronous systems, proactive recovery, state machir

5 Integrating security in a large distributed system

M. Satyanarayanan
August 1989 **ACM Transactions on Computer Systems (TOCS)**, Volume 7 Issue 3
Publisher: ACM Press
Full text available: pdf(2.90 MB) Additional Information: full citation

Andrew is a distributed computing environment that is a synthesis of the personal computing a spanning the Carnegie Mellon University campus. This paper examines the security issues that them. These mechanisms include the logical and physical separation of servers and clients, sup

6 Secure password-based cipher suite for TLS

May 2001 **ACM Transactions on Information and System Security (TISSEC)**, Vol
Publisher: ACM Press
Full text available: pdf(507.57 KB) Additional Information: full citation

SSL is the de facto standard today for securing end-to-end transport on the Internet. While the web banking. However, the adoption of password-based key-exchange protocols can overcome protocol, the standardization of SSL by IETF. The resulting protocol provides secure mutual aut

Keywords: Authenticated key exchange, dictionary attack, key agreement, password, perfect

7 A self-configuring and self-administering name system with dynamic address assignment

February 2002 **ACM Transactions on Internet Technology (TOIT)**, Volume 2 Issue 1
Publisher: ACM Press
Full text available: pdf(908.57 KB) Additional Information: full citation

In this article we present a distributed system that stores name-to-address bindings and provic services that are individually self-configuring and self-administering. The name service consists System (DNS) program. The DNS agent program automatically configures the Berkeley Interne

Keywords: Berkeley Internet Name Domain, dynamic reconfiguration, name-to-name address

8 Securing wireless applications: On securely enabling intermediary-based services and pe

Sneha Kasera, Semyon Mizikovsky, Ganapathy S. Sundaram, Thomas Y. C. Woo
September 2003 **Proceedings of the 2003 ACM workshop on Wireless security**
Publisher: ACM Press
Full text available: pdf(310.72 KB) Additional Information: full citation

Intermediary-based services and performance optimizations are increasingly being considered,

user experience of wireless mobile clients at reduced costs. However, in the presence of an enc compromising end-to-end security. We propose a new architecture to enable intermediary-base

Keywords: IPsec, end-to-end security, intermediary, mobile, performance, wireless

9 Crypto-based identifiers (CBIDs): Concepts and applications

Gabriel Montenegro, Claude Castelluccia
February 2004 **ACM Transactions on Information and System Security (TISSEC)**, Volu
Publisher: ACM Press
Full text available: pdf(262.76 KB) Additional Information: full citation

This paper addresses the identifier ownership problem. It does so by using characteristics of St calls SUCV Identifiers and Addresses, or, alternatively, Crypto-based Identifiers. Their characte SUCV addresses are particularly applicable to solve the address ownership problem that hinder

Keywords: Security, address ownership, authorization, group management, mobile IPv6, oppc

10 Authentication and integrity in outsourced databases

Einar Mykletun, Maithili Narasimha, Gene Tsudik
May 2006 **ACM Transactions on Storage (TOS)**, Volume 2 Issue 2
Publisher: ACM Press
Full text available: pdf(531.47 KB) Additional Information: full citation

In the Outsourced Database (ODB) model, entities outsource their data management needs to store, update, and access (query) their databases. This work provides mechanisms to ensure d that assure the querier that the query results have not been tampered with and are authentic (

Keywords: Outsourced databases, authentication, data authenticity, data integrity, integrity, s

11 Report of the national workshop on internet voting: issues and research agenda

C. D. Mote
May 2002 **Proceedings of the 2002 annual national conference on Digital government r**
Publisher: Digital Government Research Center
Full text available: pdf(539.99 KB) Additional Information: full citation

12 Report of the national workshop on internet voting: issues and research agenda

C. D. Mote
May 2000 **Proceedings of the 2000 annual national conference on Digital gover**
Publisher: Digital Government Research Center
Full text available: pdf(539.99 KB) Additional Information: full citation

As use of the Internet in commerce, education and personal communication has become comm adding convenience and precision, some believe that Internet voting may reverse the historical issued a memorandum in December 1999 requesting that the National Science Foundation exa

13 Virtual machine monitors: Terra: a virtual machine-based platform for trusted computing

Tal Garfinkel, Ben Pfaff, Jim Chow, Mendel Rosenblum, Dan Boneh
October 2003 **Proceedings of the nineteenth ACM symposium on Operating system**
Publisher: ACM Press
Full text available: pdf(140.31 KB) Additional Information: full citation

We present a flexible architecture for trusted computing, called Terra, that allows applications \
Applications on Terra enjoy the semantics of running on a separate, dedicated, tamper-resistar
general-purpose computing platform. Terra achieves this synthesis by use of a *trusted virtual n*

Keywords: VMM, attestation, authentication, trusted computing, virtual machine, virtual mach

14 Physical privacy: Privacy management for portable recording devices

J. Alex Halderman, Brent Waters, Edward W. Felten
October 2004 **Proceedings of the 2004 ACM workshop on Privacy in the electronic**

Publisher: ACM Press
Full text available: pdf(321.69 KB) Additional Information: full citation

The growing popularity of inexpensive, portable recording devices, such as cellular phone came
set of technologies that can be integrated into recording devices to provide stronger, more acc
consideration. Our design is based on an informed consent principle, which it supports by the u

Keywords: camera phones, privacy, recording devices

15 Internet indirection infrastructure

Ion Stoica, Daniel Adkins, Shelley Zhuang, Scott Shenker, Sonesh Surana
August 2002 **ACM SIGCOMM Computer Communication Review , Proceedings of th computer communications SIGCOMM '02**, Volume 32 Issue 4

Publisher: ACM Press
Full text available: pdf(303.69 KB) Additional Information: full citation

Attempts to generalize the Internet's point-to-point communication abstraction to provide servi
barriers. To ease the deployment of such services, this paper proposes an overlay-based Interr
Instead of explicitly sending a packet to a destination, each packet is associated with an identif

Keywords: abstraction, architecture, indirection, internet, scalable

16 Internet printing protocol (IPP) encoding and transport

Carl Kugler, Harry Lewis
December 1998 **StandardView**, Volume 6 Issue 4

Publisher: ACM Press
Full text available: pdf(399.88 KB) Additional Information: full citation, references

17 A methodology for analyzing the performance of authentication protocols

Alan Harbitter, Daniel A. Menascé
November 2002 **ACM Transactions on Information and System Security (TISSEC)**, Vol

Publisher: ACM Press
Full text available: pdf(1.25 MB) Additional Information: full citation

Performance, in terms of user response time and the consumption of processing and communic
The mix of public key and secret key encryption algorithms typically included in these protocols
develop a validated modeling methodology to be used for analyzing authentication protocol fea

Keywords: Authentication, Kerberos, mobile computing, performance modeling, proxy servers

18 Communication privacy: How to achieve blocking resistance for existing systems enabling

Stefan Köpsell, Ulf Hillig
October 2004 **Proceedings of the 2004 ACM workshop on Privacy in the electronic :**
Publisher: ACM Press
Full text available: pdf(897.66 KB) Additional Information: full citation

We are developing a blocking resistant, practical and usable system for anonymous web surfinç users in countries where the free flow of information is legally, organizationally and physically r classification of blocking criteria and some general countermeasures. Using these techniques, v

Keywords: AN.ON, JAP, Mix, blocking resistance

19 The Ω key management service

Michael K. Reiter, Matthew K. Franklin, John B. Lacy, Rebecca N. Wright
January 1996 **Proceedings of the 3rd ACM conference on Computer and communications s**
Publisher: ACM Press
Full text available: pdf(1.37 MB) Additional Information: full citation, references, citings, index terms

20 Formal methods: Proving a WS-federation passive requestor profile with a browser model

Thomas Groß, Birgit Pfitzmann, Ahmad-Reza Sadeghi
November 2005 **Proceedings of the 2005 workshop on Secure web services SWS '05**
Publisher: ACM Press
Full text available: pdf(415.13 KB) Additional Information: full citation

Web-based services are an important business area. For usability and cost-effectiveness these currently in the focus of many industrial players, is Federated Identity Managent (FIM). In this (including Microsoft Passport, OASIS SAML, and Liberty) is not yet based on rigorous proofs an

Keywords: WS-federation passive requestor profile, WSFPI, identity federation, security proof

Results 1 - 20 of 200 Result page: **1** 2 3 4 5

EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	531	713/160	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2006/10/18 11:34
L2	2227	713/168	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2006/10/18 11:35
L3	1	713/160 and (generat$5 or produc$5 or provid$5 or calculat$5) near6 (multiple or plurality or different or unique) near6 ((common or secret) keys) and ((communication) near2 (encrypt$5 or cipher$5 or scrambl$5))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2006/10/18 11:35
L4	7	713/168 and (generat$5 or produc$5 or provid$5 or calculat$5) near6 (multiple or plurality or different or unique) near6 ((common or secret) keys) and ((communication) near2 (encrypt$5 or cipher$5 or scrambl$5))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2006/10/18 11:36
L5	0	communications.clm. and unencrypted.clm. and transfer.clm. and protocol.clm. and subset.clm. and payload.clm. determin$4.clm. and secret.clm. and unique.clm. and plurality.clm. and shared.clm. and key.clm.encrypt.clm. send$4.clm. and decrypt$4.clm. and client.clm. and server.clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2006/10/18 11:40
L6	0	communications and unencrypted and transfer and protocol and subset and payload determin$4 and secret and unique and plurality and shared and key.clm.encrypt.clm. send$4 and decrypt$4 and client and server	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2006/10/18 11:41
L7	0	communications and unencrypted and transfer and protocol and subset and payload determin$4 and secret and unique and plurality and shared and key and encrypt send$4 and decrypt$4 and client and server	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2006/10/18 11:41

EAST Search History

S1	62	(encrypt$3 or cipher$3 or encipher$3 or scrambl$3) same payload same ((data transfer protocol) or (transfer protocol) or (HTTP) OR (HTTPS) or (hipertext transfer protocol))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2006/10/18 11:34
S2	62	((encrypt$3 or cipher$3 or encipher$3 or scrambl$3) same payload same ((data transfer protocol) or (transfer protocol) or (HTTP) OR (HTTPS) or (hipertext transfer protocol) or ((unencrypted or clear) transfer protocol)))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2005/06/14 05:58
S3	0	((encrypt$3 or cipher$3 or encipher$3 or scrambl$3) same ((unencrypted or clear) transfer protocol))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2005/06/14 05:58
S4	17	((x$1oring) or exclusive$1oring or ("exclusive or") or concatenat$4) near8 (random$3 or RAND) near8 (bit or number or integer or digit) near8 (public key)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2005/06/14 08:56
S5	4	hash$3 near8 ((x$1oring) or exclusive$1oring or ("exclusive or") or concatenat$4) near8 (random$3 or RAND) near8 (bit or number or integer or digit) near8 (public key)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2005/06/14 08:58
S6	61	repeatedly near3 hash$3	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2005/06/14 09:03
S7	0	repeatedly near3 hash$3 near3 ((secrete key) or (shared key))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2005/06/14 09:04
S8	0	((repeatedly or multiple) near3 hash$3) near3 ((secrete key) or (shared key))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2005/06/14 09:05
S9	0	((repeatedly or multiple) near5 hash$3) near8 ((secrete key) or (shared key))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2005/06/14 09:05

EAST Search History

S10	108	((repeatedly or multiple) near5 hash$3) near8 ((secrete key) or (shared key) or key)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2005/06/14 11:04
S11	3	(diffie$1Hellman encrypted key exchange) or ("DH$1EKE")	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2005/06/14 11:05
S13	0	((diffie$1Hellman encrypted key exchange) or ("DH$1EKE")) and payload	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2005/06/14 11:06
S14	36	(((diffie$1Hellman) same (key exchange)) or ("DH")) same payload	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2005/06/14 11:08
S15	15	(diffie$1Hellman) same (key exchange) same payload	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2005/06/14 13:40
S20	0	((bits or data) near8 ("exclusive$1or" or "exclusive$1oring" or "x$1oring" or "x$1or"))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2005/06/14 13:45
S26	313	(exclusive$1or or exclusive$1oring or x$1or or x$oring) near8 (bits or digits) and HTTP	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2005/06/14 13:48
S27	1	713/162.ccls. and (exclusive$1or or exclusive$1oring or x$1or or x$oring) near8 (bits or digits) and HTTP	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2005/06/14 14:18
S28	1	"09950927"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2005/11/14 13:01
S30	0	((multiple or plurality or many) near5 payloads) same (unique near5 key)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2005/11/15 08:33

EAST Search History

S31	32	((multiple or plurality or many) near5 payloads) and (unique near5 key)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2005/11/15 08:33
S32	2	"20050254645".pn.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2005/12/30 11:54
S34	108	nonce near encrypt$4	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2006/03/10 10:44
S35	0	disest access authentication	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2006/03/10 11:29
S36	126	(different near4 key) near9 (encrypt$4 or cipher$4 or encipher$4) near9 (session)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2006/03/10 11:31
S37	113	(different near4 key) near4 (encrypt$4 or cipher$4 or encipher$4) near9 (session)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2006/03/10 11:31
S38	84	(different near2 key) near4 (encrypt$4 or cipher$4 or encipher$4) near9 (session)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2006/03/10 11:39
S39	2	"09928469"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2006/03/10 11:39
S40	1256	(generat$5 or produc$5 or provid$5 or calculat$5) near10 (multiple or plurality or different or unique) same ((common or secret) keys)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2006/08/01 14:55

EAST Search History

S41	125	(generat$5 or produc$5 or provid$5 or calculat$5) near10 (multiple or plurality or different or unique) same ((common or secret) keys) and (session near2 (encrypt$5 or cipher$5 or scrambl$5))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2006/08/01 15:20
S42	54	(generat$5 or produc$5 or provid$5 or calculat$5) near6 (multiple or plurality or different or unique) near6 ((common or secret) keys) and (session near2 (encrypt$5 or cipher$5 or scrambl$5))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2006/08/01 15:38
S43	167	(generat$5 or produc$5 or provid$5 or calculat$5) near6 (multiple or plurality or different or unique) near6 ((common or secret) keys) and ((communication or session) near2 (encrypt$5 or cipher$5 or scrambl$5))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2006/08/03 10:09
S44	2	"20020147870".pn.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2006/08/01 15:39
S45	129	(generat$5 or produc$5 or provid$5 or calculat$5) near6 (multiple or plurality or different or unique) near6 ((common or secret) keys) and ((communication) near2 (encrypt$5 or cipher$5 or scrambl$5))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2006/08/03 10:09